INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 3, Numărul 1, Martie 2024

Componentele războiului electronic – Strategii și tehnici

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Componentele războiului electronic – Strategii și tehnici, *Intelligence Info*, **3**:1, 11-21, DOI: 10.58679/II38042, https://www.intelligenceinfo.org/componentele-razboiului-electronic-strategii-si-tehnici/

Publicat online: 06.01.2024

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Componentele războiului electronic – Strategii și tehnici

Ing. fiz. Nicolae SFETCU, MPhil[1]
nicolae@sfetcu.com

Components of Electronic Warfare – Strategies and Techniques

Abstract

Activities used in electronic/electromagnetic warfare include electro-optical, infrared, and radio frequency countermeasures; electromagnetic compatibility and deception; radio jamming, radar jamming and deception, and electronic (or anti-jamming) countermeasures; electronic masking, probing, reconnaissance and intelligence; electronic security; EW reprogramming; emissions control; spectrum management; and wartime backup modes. Traditional electronic warfare has three main components.

Keywords: electronic warfare, electromagnetic warfare, electronic attack, electronic countermeasures, electronic protection, electronic countermeasures, electronic support, electronic support measures

Rezumat

Activitățile utilizate în războiul electronic/electromagnetic includ contramăsuri electro-optice, în infraroșu și frecvență radio; compatibilitatea electromagnetică și decepția; bruiaj radio, bruiaj și decepție radar, și contramăsuri electronice (sau anti-bruiaj); mascare electronică, sondare, recunoaștere și informații; securitate electronică; reprogramare EW; controlul emisiilor; managementul spectrului; și modurile de rezervă în timp de război. Războiul electronic tradițional are trei componente principale.

Cuvinte cheie: război electronic, război electromagnetic, atacul electronic, contramăsuri electronice, protecția electronică, contra-contramăsuri electronice, suportul electronic, măsuri de asistență electronică

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

INTELLIGENCE INFO, Volumul 3, Numărul 1, Martie 2024, pp. 11-21
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II38042
URL: https://www.intelligenceinfo.org/componentele-razboiului-electronic-strategii-si-tehnici/
© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Articol în Acces Deschis (Open Access) distribuit în conformitate cu termenii licenței de atribuire Creative Commons CC BY SA 4.0
(https://creativecommons.org/licenses/by-sa/4.0/)

Introducere

Activitățile utilizate în războiul electronic/electromagnetic (EW) includ contramăsuri electro-optice, în infraroșu și frecvență radio; compatibilitatea electromagnetică și decepția; bruiaj radio, bruiaj și decepție radar, și contramăsuri electronice (sau anti-bruiaj); mascare electronică, sondare, recunoaștere și informații; securitate electronică; reprogramare EW; controlul emisiilor; managementul spectrului; și modurile de rezervă în timp de război[2]. Războiul electronic tradițional are trei componente principale:

Atacul electronic (EA)

Atacul electronic (EA) este „acea diviziune a războiului electronic care implică utilizarea energiei electromagnetice, a energiei dirijate sau a armelor antiradiații pentru a ataca personal, instalații sau echipamente cu intenția de a degrada, neutraliza sau distruge capacitatea de luptă a inamicului și este considerat o formă de tras cu arma”[3]. Atacul electronic folosește bruiajul electromagnetic punctual, bruiajul de baraj și baleierea, folosind tehnici de decepție electromagnetică precum fi ținta falsă sau generarea de ținte duplicate.

Atacul electronic (EA), cunoscut și sub denumirea de contramăsuri electronice (ECM), implică utilizarea ofensivă a armelor cu energie electromagnetică, cu energie dirijată, sau a armelor antiradiații, pentru a ataca și perturba adversarul prin „blocare” pe sisteme de comunicații sau radar. Armele anti-radiații includ rachete sau bombe care țintesc

[2] (Army 2020, i, v–x)
[3] (Army 2016)

un anumit semnal (radio sau radar) pentru a distruge sistemul de difuzare.Obiectivele operaționale ale ECM sunt:

- Contracararea ESM și sistemelor de comunicații ostile.
- Introducerea de date false sistemele electronice ostile.
- Distrugerea sistemului de război electronic ostil.

Contramăsurile electronice se pot clasifica în contramăsuri electro-optice-infraroșu (CM EO-IR) (bruiaj cu laser, fum/aerosoli, suprimatoare de semnături, momeli, produse pirotehnice/piroforice, lasere de înaltă energie sau contramăsuri de energie IR direcționată) și contramăsuri de frecvență radio (de exemplu, arme ghidate de precizie sau controlate radio, echipamente de comunicații și sisteme de senzori).

Pentru aceasta , sunt folosite diverse tehnici specifice, care pot fi clasificate în ECM active și ECM pasive. ECM active implică degradarea eficacității sistemelor de război electronic ale inamicului prin generarea și transmiterea de energie electromagnetică, prin bruiaj de zgomot și bruiaj deceptiv[4].

Bruiajul de zgomot injectează semnale de interferență în sistemul electronic al inamicului, astfel încât semnalul țintă să fie mascat sau complet bruiat de interferență. Există tehnici diferite pentru a genera interferențe[5], precum bruiajul punctual (Spot Jamming) concentrat pe o bandă foarte îngustă de frecvență, bruiajul de baleiaj (Sweep Jamming) care mătură întreaga frecvență, sau bruiajul de baraj (Barrage Jamming) care vizează mai multe frecvențe simultan.

Bruiajul deceptiv produc poziții și viteze false ale țintei prin pseudo-semnale, prin tehnici manipulative, sau imitative (introducerea de radiații EM în canalele inamice care imită propria lor emisie se numește decepție imitativă)[6]. Tehnicile manipulative modifică radiațiile electromagnetice prietenoase pentru a păcăli adversarul, prin generarea de ținte false, falsificarea gamei de frecvențe, a vitezei și unghiului[7][8]. Generarea țintelor false se folosește împotriva radarelor, avertizare timpurie și interceptarea controlului la sol, pentru

[4] (Neri 1991)
[5] (Butt și Jalil 2013)
[6] (Singh 1988)
[7] (Martino 2012)
[8] (Butt și Jalil 2013)

a deruta operatorul de radar inamic[9] care nu va putea face distincția între ținte false și ținte reale[10]. Falsificarea razei, vitezei și unghiului exploatează vulnerabilitățile de monitorizare ale inamicului[11].

ECM pasiv folosește reflectoare de confuzie pentru înșelarea sistemelor electronice ale inamicului, prin mijloace chimice (utilizarea fumului și agenților chimici precum aerosolii[12]) sau mecanice (utilizarea de obiecte mecanice special concepute, precum ”pleava” alcătuită din fibre dielectrice subțiri acoperite cu metal[13]. ECM ofensive iau adesea forma bruiajului, pe când cele de auto-protecție (defensive) includ utilizarea îmbunătățirii blip-ului și blocarea terminalelor de rachetă.

În cazul radarelor, strategiile ECM includ interferența radarului, modificările țintei și modificarea proprietăților electrice ale aerului, prin tehnici de interferență precum bruiajul și decepția[14]. Bruiajul radio sau blocajul comunicațiilor perturbă comunicațiile prin scăderea raportului semnal-zgomot.

Protecția electronică (EP)

Protecția electronică (EP) este „acea diviziune a războiului electronic care implică mijloace pasive și active luate pentru a proteja personalul, facilitățile și echipamentele împotriva oricăror efecte ale angajării prietenești sau inamice a războiului electronic care degradează, neutralizează sau distrug capacitatea de luptă amicală”[15].

Protecția electronică, cunoscută și ca măsură de protecție electronică (EPM) în Europa, sau contra-contramăsura electronică (ECCM), se concentrează pe protejarea sistemelor electronice împotriva atacurilor prin înfrângerea bruiajului inamic. Aceasta implică utilizarea tehnicilor de criptare, salt de frecvență și întărire pentru a proteja sistemele critice, folosind tehnologiile cu spectru extins, utilizarea listelor de frecvențe

[9] (Rahman 2019)
[10] (Brunt 1978)
[11] (Martino 2012)
[12] (Rahman 2019)
[13] (Grant și Collins 1982)
[14] (Polmar 1979)
[15] (Army 2016)

restricționate, controlul emisiilor (EMCON) și tehnologia cu observabilitate scăzută (stealth)[16][17].

Protecția electronică, cunoscută și sub numele de contra-contramăsuri electronice (ECCM), folosește tactici de război electronic (EWTR) și tehnici încorporate în proiectarea echipamentelor electronice pentru a anihila ECM inamice care implică tehnici de bruiaj și decepție. Domeniile exploatate în mod obișnuit de ECCM sunt:

- *ECCM spațiale*, precum anulator de lobi laterali, obturarea lobului lateral, sau tehnica de ardere[18][19].
- *ECCM spectrale* (bazate pe frecvență), precum tehnica cu probabilitate scăzută de interceptare, agilitatea în frecvență, sau filtrarea Doppler[20][21].
- *ECCM temporale* (tehnici dependente de timp), inclusiv extensiune-compresie puls, agilitatea pulsurilor de radiofrecvență, dickefix, sau rata constantă de alarmă falsă[22][23].
- *ECCM prin rețea radar*, o combinație de cel puțin două sau trei radare care furnizează informații către un hub central[24].

Suport electronic (ES)

Suportul războiului electronic (ES) este „divizia războiului electronic care implică acțiuni însărcinate sau sub controlul direct al unui comandant operațional să caute, să intercepteze, să identifice și să localizeze surse de energie electromagnetică radiată intenționată și neintenționată în acest scop, de recunoaștere imediată a amenințărilor, țintire, planificare și desfășurare a operațiunilor viitoare”[25]. Caracteristicile ES[26]:

- Este utilizat în timp de pace, criză și război, ceea ce contribuie la construirea unei baze de date EW/informații pentru planificare și operațiuni.
- Oferă o capacitate de culegere de informații pentru orice vreme, zi/noapte, pe distanță lungă.
- Exploatează emisiile electromagnetice ale unui inamic și poate oferi informații despre capabilitățile și intențiile inamicului.

[16] (Army 2020)
[17] (Tsui 2022)
[18] (Neri 1991)
[19] (Grant și Collins 1982)
[20] (Grant și Collins 1982)
[21] (Skolnik 2008)
[22] (Grant și Collins 1982)
[23] (Skolnik 2008)
[24] (Sharma, Sarma, și Mastorakis 2020)
[25] (Army 2016)
[26] (US Marine Corps 2016)

- Este ascuns și pasiv.
- Este o metodă neintruzivă de colectare a informațiilor.

Sistemele de sprijin pentru războiul electronic colectează date și produc intelligence pentru[27]:

- Coroborarea cu alte surse de intelligence.
- Operațiuni directe EA.
- Măsuri de autoprotecție.
- Sisteme de arme pentru distrugerea fizică.
- Sprijinirea eforturilor PE.
- Crearea sau modificarea de baze de date EW.
- Activități de asistență pentru operațiuni de informare (IO).

Suportul pentru războiul electronic (ES), prin măsurile de asistență electronică (ESM), implică colectarea și analiza semnalelor electromagnetice emise de adversari pentru a detecta, intercepta, identifica, și/sau localiza sursele de energie electromagnetică radiată. Acest lucru oferă informații și conștientizare a situației, ajutând comandanții în luarea deciziilor. Măsurile de asistență electronică urmăresc recunoașterea imediată a amenințărilor, activitate denumită informații, supraveghere și recunoaștere (ISR) sau informații, supraveghere, achiziție de ținte și recunoaștere (ISTAR)[28]. Inteligența semnalelor (SIGINT), care se suprapune parțial cu ES, analiză și identifică transmisiile din surse precum comunicațiile radio, telefoanele mobile, radarul sau comunicațiile cu microunde[29]. SIGINT se compune din inteligența electronică (ELINT - compilează date operaționale) și inteligența de comunicații (COMINT - comunicarea adversarilor) și receptorul ESM. ESM are un scop tactic care necesită acțiuni imediate, în timp ce SIGINT colectează date de informații pentru o analiză ulterioară sau în timp nereal[30].

Funcțiile cheie ale sistemelor ESM sunt: interceptarea, identificarea, analizarea și localizarea surselor de radiații electromagnetice ostile în scopul recunoașterii și angajării tactice a forțelor, eventual printr-un ordin electronic de luptă (EOB), inclusiv prin operațiuni ECM și ECCM.

[27] (US Marine Corps 2016)
[28] (Kjellén 2018)
[29] (Kjellén 2018)
[30] (Rahman 2019)

ESM măsoară parametrii semnalului radar de intrare în intervalul de frecvență de funcționare: lățimea impulsului, frecvența de repetare a impulsurilor, puterea semnalului, ora de sosire, direcția de sosire, etc.[31], fiind format din: antene, receptoare, procesor de semnal, computer cu bibliotecă de emițători și unitate de afișare[32]. Receptorul ESM are cea mai mare influență asupra caracteristicilor sistemului ESM[3334].

Măsurile de suport electronic pot oferi detectarea inițială sau cunoașterea sistemelor străine, o bibliotecă de date tehnice și operaționale privind sistemele străine, și informații de luptă tactică în care se utilizează acea bibliotecă[35].

Caracteristicile de dorit pentru echipamentele de supraveghere și colectare electromagnetică includ

- capacitatea de spectru larg sau de lățime de bandă, deoarece frecvențele străine sunt inițial necunoscute,
- interval dinamic larg, deoarece puterea semnalului este inițial necunoscută,
- trecere de bandă îngustă pentru a discrimina semnalul de interes de la alte radiații electromagnetice pe frecvențele apropiate, și
- măsurarea bună a unghiului de fugă pentru a localiza transmițătorul[36].

De obicei, sunt necesare mai multe receptoare pentru supravegherea întregului spectru.

Tehnici și tactici

Principalele activități utilizate în EW includ următoarele[37]: contramăsuri, managementul de lupte EM (EMBM), compatibilitatea EM; înșelăciune EM; întărirea EM, rezoluție interferență EM, intruziune EM, bruiaj EM, EMP, control spectru EM, colectare de inteligență electronică, mascare electronică, sondare electronică, recunoaștere electronică, securitate electronică, reprogramare EW, control emisii, JEMSO, JEMSMO, observabilitate/ascundere scăzută, interceptarea și retransmiterea semnalelor, navigație război (NAVWAR), geolocalizare de precizie și moduri de rezervă în timp de război.

[31] (Li et al. 2018)
[32] (Shankar și Mohan 2013)
[33] (Martino 2012)
[34] (Sharma, Sarma, și Mastorakis 2020)
[35] (Polmar 1979)
[36] (Polmar 1979)
[37] (Army 2020)

EW include o serie de tehnici și tactici, inclusiv[38]: bruiaj, falsificare, energie direcționată (DE), război electronic cibernetic (CEW) și înșelăciune electronică.

- **Bruiaj**: radiația deliberată EM pentru a preveni sau reduce utilizarea eficientă a EMS de către un inamic[39].
- **Falsificarea**: transmiterea de informații false către senzorii sau sistemele de comunicare ale adversarului, provocând confuzie și potențial să-i determine să ia decizii incorecte[40].
- **Energie direcționată**: este „un termen umbrelă care acoperă tehnologiile care se referă la producerea unui fascicul de energie electromagnetică concentrată sau a particulelor atomice sau subatomice”[41]. O armă cu energie direcționată folosește „energia dirijată în primul rând ca mijloc direct de a deteriora sau distruge echipamentul, instalațiile și personalul inamicului” [42]. Energia direcționată folosește tehnologiile care produc energie EM concentrată și particule atomice sau subatomice, ca mijloc de a incapacita, deteriora, dezactiva sau distruge echipamentele, instalațiile și/sau personalul inamic.
- **Război electronic cibernetic**: îmbină capacitățile spațiului cibernetic cu metodele tradiționale EW, prin infiltrarea în computerul sau în sistemele de comunicații ale unui adversar pentru a fura sau manipula informații și pentru a-i perturba operațiunile[43].
- **Decepția electronică**: folosirea mijloacelor electronice pentru a induce în eroare un adversar să creadă ceva neadevărat, prin tehnici precum crearea de ținte false pe ecranele radar, utilizarea contramăsurilor electro-optice, infraroșu sau frecvență radio și transmiterea de semnale false pentru a deruta senzorii adversarului[44].
- **Armele antiradiație**: folosesc energia radiată emisă de țintă ca mecanism de ghidare către un emițător vizat (de exemplu, sistemul de rachete antiradiații de mare viteză [HARM - high-speed antiradiation missile]).

Managementul spectrului include „planificarea, coordonarea și gestionarea utilizării în comun a spectrului electromagnetic prin proceduri operaționale, de inginerie și administrative. Obiectivul managementului spectrului este de a permite sistemelor electronice să își îndeplinească funcțiile în mediul vizat, fără a provoca sau a suferi interferențe inacceptabile”[45].

[38] (Duke 2023)
[39] (Army 2020)
[40] (Army 2020, I–10)
[41] (Army 2016)
[42] (Army 2016)
[43] (Yasar, Yasar, și Topcu 2012)
[44] (Adamy 2001)
[45] (Army 2016)

EW este folosit pentru a crea efecte decisive, autonome sau pentru a sprijini operațiunile militare prin generarea diferitelor niveluri de control, detecție, negare, înșelăciune, perturbare, degradare, exploatare, protecție și distrugere.

- În *războiul neregulat*, EW poate influența adversarul, populația prietenoasă și populația neutră, cu mesajul operațiunilor de informare (IO).
- În *operațiunile informaționale*, EW contribuie prin folosirea tacticilor și tehnicilor ofensive și defensive pentru a modela, perturba și exploata utilizarea adversă a EMS, protejând în același timp libertatea de acțiune amicală.
- În *operațiunile spațiale*, manevrele fizice și colectarea EM necontestată implică o formă de EW.
- În operațiunile în *spațiul cibernetic* este necesară utilizarea EMS pentru activarea efectelor, prin coordonarea cu EW.
- În războiul *prin navigație*, EW produce efecte NAVWAR prin influențarea transmisiei sistemului global de navigație prin satelit sau a altor semnale radio.

Alte tehnici și tactici folosite în EW[46]:

- *Managementul bătăliilor electromagnetice (EMBM)*: monitorizarea dinamică, evaluarea, planificarea și conducerea operațiunilor.
- *Compatibilitate electromagnetica (EMC)*: capacitatea sistemelor, echipamentelor și dispozitivelor de a funcționa fără a suferi o degradare inacceptabilă sau a provoca o degradare neintenționată.
- *Decepția electromagnetică*: radiația deliberată, reradierea, alterarea, suprimarea, absorbția, negarea, îmbunătățirea sau reflectarea energiei EM într-o manieră menită să transmită informații deceptive unui inamic.
- *Întărirea electromagnetică*: pentru a proteja împotriva efectelor nedorite ale energiei EM.
- *Rezoluția interferențelor electromagnetice*: procesul de diagnosticare sistematică a cauzei sau sursei interferențelor EM.
- *Intruziune electromagnetică*: inserarea intenționată a energiei EM în căile de transmisie pentru a înșela operatorii sau a provoca confuzie.
- *Blocaj electromagnetic*: modificarea energiei EM pentru a preveni sau reduce utilizarea eficientă a EMS de către un inamic.
- *Puls electromagnetic (EMP)*: un impuls electronic puternic produs de o explozie nucleară sau generat în mod convențional, care produce supratensiuni.
- *Controlul spectrului electromagnetic*: prin execuția coordonată a JEMSO cu alte operațiuni letale și neletale care afectează EMOE.
- *Inteligența electronică (ELINT)*: o subcomponentă a SIGINT
- *Mascarea electronică*: radiația controlată a energiei EM pe frecvențele prietenoase care să protejeze emisiile sistemelor electronice de comunicații prietenoase
- *Sondarea electronică*: radiația intenționată concepută pentru a fi introdusă în dispozitivele sau sistemele potențialilor inamici.

[46] (Army 2020)

- *Recunoașterea electronică*: detectarea, localizarea, identificarea și evaluarea radiațiilor EM străine.
- *Securitatea electronică*: protecția împotriva persoanelor neautorizate în interceptarea și studiul radiațiilor EM.
- *Reprogramarea războiului electronic*: modificarea EW sau a sistemelor de detectare a țintei (TSS) ca răspuns la modificările validate ale echipamentelor, tacticilor sau EME.
- *Controlul emisiilor*: utilizarea selectivă și controlată a emițătorilor pentru a optimiza capabilitățile C&C minimizând în același timp detecția de către senzorii inamici, interferența reciprocă între sistemele prietenoase și interferența inamicului.
- *Operații comune cu spectrul electromagnetic (JEMSO)*: eforturile coordonate de a exploata, ataca, proteja și gestiona EMOE pentru a atinge obiectivele.
- *Operațiuni comune de gestionare a spectrului electromagnetic (JEMSMO)*: planificarea, coordonarea și gestionarea utilizării comune a EMS prin proceduri operaționale, de inginerie și administrative.
- *Observabilitate scăzută/Infiltrare*: EP cu observabilitate scăzută/stealth, pentru a opera prin reducerea posibilității de detectare de către adversari.
- *Meaconing*: recepționarea semnalelor de radiofar și redifuzarea lor pe aceeași frecvență pentru a încurca navigarea
- *Războiul naval (NAVWAR)*: acțiuni deliberate pentru asigurarea și prevenirea informațiilor specifice navale.
- *Geolocalizare de precizie*: planificarea, coordonarea și gestionarea activelor prietenoase pentru geolocalizarea sistemelor RF inamice.
- *Moduri de rezervă în timp de război (WARM)*: caracteristici și proceduri de operare care vor contribui la eficacitatea militară dacă nu sunt cunoscute sau înțelese greșit de comandanții oponenți înainte de a fi utilizate, dar ar putea fi exploatate sau neutralizate dacă sunt cunoscute dinainte.

Concluzie

În peisajul cu evoluție rapidă a războiului modern, componentele de război electronic au devenit instrumente indispensabile pentru a obține un avantaj decisiv pe câmpul de luptă. De la strângerea de informații prin ESM și SIGINT până la perturbarea sistemelor inamice cu ECM și apărarea împotriva atacurilor electronice cu ECCM, aceste componente contribuie colectiv la superioritatea forțelor militare în spectrul electromagnetic. Pe măsură ce tehnologia continuă să avanseze, războiul electronic va rămâne un domeniu dinamic și critic, modelând rezultatul conflictelor și asigurând securitatea națiunilor.

Bibliografie

Adamy, David. 2001. *EW 101: A First Course in Electronic Warfare*. Artech House.

Army, United States Government US. 2016. „Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms". https://irp.fas.org/doddir/dod/jp1_02.pdf.

———. 2020. *Joint Publication JP 3-13 Information Operations Change 1 November 2014*. Independently Published.

Brunt, Leroy B. Van. 1978. *Applied ECM*. EW Engineering.

Butt, Faran, și Madiha Jalil. 2013. *An overview of electronic warfare in radar systems*. https://doi.org/10.1109/TAEECE.2013.6557273.

Duke, Audrey. 2023. „Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations". https://apps.dtic.mil/sti/citations/AD1206172.

Grant, P. M., și J. H. Collins. 1982. „Introduction to Electronic Warfare". *IEE Proceedings F (Communications, Radar and Signal Processing)* 129 (3): 113–32. https://doi.org/10.1049/ip-f-1.1982.0020.

Kjellén, Jonas. 2018. „Russian Electronic Warfare - The role of Electronic Warfare in the Russian Armed Forces". https://web.archive.org/web/20181010174505/https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C4c547bec-bdfa-4bdb-a1c9-018097aaf615.pdf.

Li, Xueqiong, Zhitao Huang, Fenghua Wang, Xiang Wanga, și Tianrui Liu. 2018. „Toward Convolutional Neural Networks on Pulse Repetition Interval Modulation Recognition". *IEEE Communications Letters* PP (august): 1–1. https://doi.org/10.1109/LCOMM.2018.2864725.

Martino, Andrea De. 2012. *Introduction to Modern EW Systems*. Artech House.

Neri, F. 1991. „Introduction to electronic defense systems". În . https://www.semanticscholar.org/paper/Introduction-to-electronic-defense-systems-Neri/8d8aed6d92ecf7af850f09a2ee740380c2d4b366.

Polmar, Norman. 1979. „The U. S. Navy: Electronic Warfare (Part 2)". U.S. Naval Institute. 1 noiembrie 1979. https://www.usni.org/magazines/proceedings/1979/november/u-s-navy-electronic-warfare-part-2.

Rahman, H. 2019. *Introduction to Electronic Defense Systems*. Boca Raton, FL, USA: CRC Press.

Shankar, M., și B. Mohan. 2013. „Recent Advances in Electronic Warfare-ESM Systems". În . https://www.semanticscholar.org/paper/RECENT-ADVANCES-IN-ELECTRONIC-WARFARE-ESM-SYSTEMS-Shankar-Mohan/bf6e4c372514695dd167eebf6f9dfb78ca120f6a.

Sharma, Purabi, Kandarpa Kumar Sarma, și Nikos E. Mastorakis. 2020. „Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications". *IEEE Access* 8: 224761–80. https://doi.org/10.1109/ACCESS.2020.3044453.

Singh, Mohinder. 1988. „Electronic Warfare". https://www.drdo.gov.in/sites/default/files/publcations-document/Electronic%20Warfare.pdf.

Skolnik, Merrill I. 2008. *Radar Handbook, Third Edition*. McGraw-Hill Education.

Tsui, Chi-Hao Cheng, James. 2022. *An Introduction to Electronic Warfare; from the First Jamming to Machine Learning Techniques*. New York: River Publishers. https://doi.org/10.1201/9781003337171.

US Marine Corps. 2016. „Electronic Warfare". https://www.marines.mil/Portals/1/Publications/MCRP%203-32D.1%20(Formerly%20MCWP%203-40.5).pdf.

Yasar, Nurgul, Fatih Mustafa Yasar, și Yucel Topcu. 2012. „Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield". În *Cyber Sensing 2012*, 8408:151–59. SPIE. https://doi.org/10.1117/12.919454.